Retail and Rational Responses to RFID Privacy Concerns

Richard J. H. Varn

Technology Policy Advisor

National Retail Federation

Negative Policy Issues

- Data mining and matching
- Surveillance and tracking
- Privacy invasion
  - Government
  - Private party

Negative Policy Issues

- Criminal use of personal data
- Annoying or invasive marketing
- Job loss from technology
- Environmental effects of chips in the trash
- FUD of the unknown

Positive Policy Issues

- Economic growth, productivity, and new business development

- Lower cost of doing business

- Customer convenience

- Better service

- National competitiveness
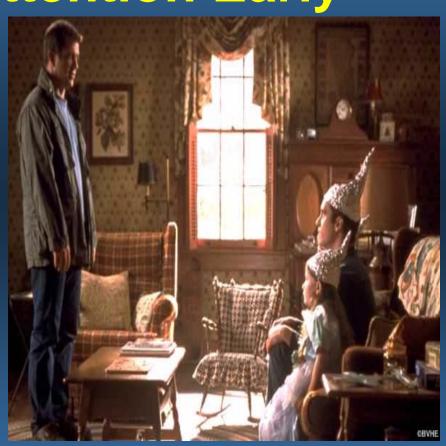
- More accurate economic data

Positive Policy Issues

- Better product recalls

- Crime prevention, investigation, apprehension, and punishment

- Support anti-terrorism efforts

- Safer products, food, and medicine

- Lower cost for recycling and reuse

Why the Negative Has Gotten More Attention Early

- It is technical, so it is hard to tell a nut from a prophet
- Privacy advocates use every new technology to raise old privacy issues
- There is confusion
- Some concerns are legitimate

Retail RFID

Before, In, and Out of the Store

First, Pre-RFID

- Anti-theft tags

- Loss prevention programs with monitoring, cameras, and personnel

- Retailers casually and sometimes systematically watch how customers shop to improve marketing, sales, and service

- Quality control though paid shoppers

First, Pre-RFID

- Retailer owned data comes from many sources such as store credit, loyalty programs, and records of sales

- Data about one's own customers is a key competitive advantage and is closely and jealously guarded

Before the Store

- Supply chain management
- Distribution logistics and reverse logistics
- Just in time supply
- Stock room and receiving automation
- Streamline the flow of goods and cut down on friction, waste, and errors
- Optimize the retail economy

In the Store

- Help the shopper find what is here and where it is

- Know what needs to be restocked in real time

- Self-check out

- Smart carts with sign up process similar to loyalty card

- Reduce theft

- Most EPC tags will be removable

Out of the Store

- It is illegal to read an RFID tag without permission in nearly every state and illegal to do so in order to harm someone in all states

- Computer crime laws prohibit access to computers including RFID chips, data, and electronic communications without permission in general and specifically ban such use when done to harm persons or property (including data)

Out of the Store

- Retail is limited to reading, by permission only, tags brought back to the store
- Receipt-less returns, can I have more like this, what goes with this, or other services
- Home uses for tags in, on, or attached to products
- End of life uses

RFID Policy Framework

A Rational Approach to Address the Issues

A Rational Approach

- Note: this is not the path taken so far

- Review one's current laws

- Identify the gaps

- Determine the proper level of government at which any gaps should be addressed

A Rational Approach

- Draft legislation and/or rules narrowly and accurately

- Use sunrise and sunset clauses as appropriate

A Rational Approach

- Prohibit the undesired behaviors, not the technology

- Determine the punishment and method for enforcement

- Differentiate between four different kinds of RFID deployments

A Rational Approach

- Four kinds of RFID deployments:
  - Government documents and devices transferred to the public
  - Government documents and devices internal to government
  - Private documents and devices transferred to the public
  - Private documents and devices internal to a private entity

Government Documents/Devices to Public

Policy Question	Government Documents and Devices Transferred to the Public and Use Is Mandatory	Government Documents and Devices Transferred Where Citizens Knowingly Choose to Use It
Should tracking be allowed?	No. Tracking without consent or operation of law should be forbidden	No. Tracking without consent or operation of law should be forbidden
Does remote reading require explicit consent or operation of law?	Always	Yes unless varied by the terms of any agreement of use or participation
Where should this policy issue be addressed?	In statute	In statute
Notice of presence of remote reading capability required?	Yes	Yes

Government Documents/Devices Internal

Policy Question	Government Documents and Devices Transferred to Government Employees for Their Use	Government Documents and Devices In Use in Government to Track Objects (documents, inventory, animals, etc.)
Should tracking be allowed?	Tracking for non-work purposes should be forbidden but tracking for work purposes depends on employment law and contracts (if any)	Tracking is the purpose of the use of the technology so tracking is allowed, but may not be incidentally be used to track a person in contradiction of the limits in the other three categories
Does remote reading require explicit consent or operation of law?	Depends on employment laws and rules governing public employees	Never
Where should this policy issue be addressed?	In statute	In statute
Notice of presence of remote reading capability required?	Yes	Yes

Policy Question	Documents and Devices Sold With RFID or Remote Reading Capability as an Explicit Part of the Function of the Document or Device	Documents and Devices Sold or Given Away With RFID or Remote Reading Capability In, On, or Attached to the Product
Should tracking be allowed?	No. Tracking without consent or operation of law should be forbidden	No. Tracking without consent or operation of law should be forbidden
Does remote reading require explicit consent or operation of law?	No	Yes (already covered by state law) unless done incidentally as a result of another legitimate use of the technology and no data is retained or used
Where should this policy issue be addressed?	Tracking issues needs to be clarified by statute	In statute
Notice of presence of remote reading capability required?	No as it is inherent in the product	Unnecessary and of little or no benefit

Policy Question	Documents and Devices Transferred to Private Employees for Their Use	Documents and Devices In Use by Private Persons to Track Objects (inventory, animals, etc.)
Should tracking be allowed?	Tracking for non-work purposes should be forbidden but tracking for work purposes depends on employment law and contracts (if any)	Tracking is the purpose of the use of the technology so tracking is allowed, but may not be incidentally be used to track a person in contradiction of the limits in the other three categories
Does remote reading require explicit consent or operation of law?	Depends on employment laws and rules governing employees	No
Where should this policy issue be addressed?	In statute as needed, rules, and contracts	No legislative action required
Notice of presence of remote reading capability required?	Depends on employment laws and rules governing employees	No

Current Legislative Approach

- Broad based bans, limitations, and requirements

- Overbroad definitions that cover commonly used technologies including non-RFID technologies

- Interlocking and overlapping definitions that have broad and unintended effect

Legislative Approach

- Language focusing on technology rather than behavior
- Current applicable statutes are ignored
- Language seeks to codify private codes of conduct
- Language based on false or unsupported assumptions

Some Sources of Confusion

- Advocates assert RFID uses as inevitable even though such uses are unconstitutional, illegal, physically impossible, or unfit for the stated purpose
- Many suggested "inevitable" uses would cause customers to refuse to patronize, sue, and bankrupt any retailer who would employ them

Some Sources of Confusion

- All patents applications are assumed to be implementation plans

- Also asserted are data mining and matching concerns that are either already true or are far broader than RFID and would involve a complete rewrite of our privacy laws

Conclusion: Focus on the Difference

- We cannot let every new technology force us to re-open everything

- What is new and different?

- Legislate bad acts and actors

- Proactively protect privacy and keep customers in the loop and in the know

- Market the benefits, address the negatives, debunk the myths

Conclusion: Focus on the Difference

- Underneath many new technologies is just a new way to use a database

- Do current laws and policies deal with it adequately?

- Narrowly tailor the response to the difference, not the technology itself